



Market Analyst Briefing 4Q2020

Tim Bradford
Co-Founder, CEO

Charles Herring
Co-Founder, CTO

WitFoo Mission & Research Areas

WitFoo is dedicated to creating data and tools that accelerate maturity in the craft of cybersecurity operations.

1. Investigators do not understand what their tools are saying
2. Managers cannot track security practice success
3. Security practice cannot express value to business
4. Security vendors cannot be held accountable
5. Organizations cannot safely share information with each other
6. Organizations cannot safely report crimes to law enforcement
7. Law enforcement lacks evidence to prosecute criminals

Precinct 6.0

Precinct 6.1

WitFoo Progress

- Stealth Mode (2016)
 - Product tested live on University of Chicago networks
 - Validated Intellectual Property & Methodology
- Scrimmage Mode (2017 – 2020)
 - Expanded to 30+ networks
 - 3,000+ experiments ran
 - 6 Platform Overhauls (big data issues & expansion of scope)
 - Tested messaging & function with Partners, Prospects and Analysts
 - Recruit and Train Distribution, Resell and Technology Partners
- Business Launch (2021)

Precinct - World's First Diagnostic SIEM



Diagnostic Reporting

Assisted Investigations

Automated Analysis

Modus Operandi

Graph Theory

Normalized Data

Natural Language Processing

- Holistic Analysis
- No Parsers
- No Rules
- Retro IOC Analysis
- Infinite Big Data
- Normalized Data
- “Kill-chain” Incidents
- Automated Enrichment
- Manual Response
- Reduced MTTR
- Reduced Work Units
- **Preventative Diagnostics**

Why Customers Purchase Precinct

Log Storage &
Search

Business Metrics

Improve SECOPS

Predictive
Diagnostics

SIEM Cost
Reduction

CMMC Compliance

SOAR

MSSP Operations

Cloud Monitoring

Procurement
Competitive Bid

Vendor
Requirement

Solving Craft Problems

WitFoo Artifact	Codeless SOAR	General Accounting Principles	DC Aware & Load Balanced		Partner MSSP
NLP Message Comprehension	WitFoo Incident	Personnel Effectiveness	Extreme Compression		Partner Hosted SaaS
OpenAPI / STIX Support	Automated Analysis	Tool Effectiveness	IOPS Optimized	Aggregator Mode (Federation)	Cloud Hosted
Automatic Parsing	Modus Operandi Stitching	Compliance Readiness	Infinite Scale	Global IOC Feed	Hypervisor

Integration Management

Reduced MTTK & MTTR

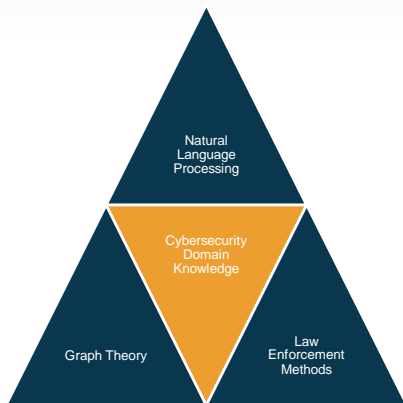
Speaking Business Language

Big Data

Safely Share Intel

Deployment Flexibility

Diagnostic SIEM - Data Evolution



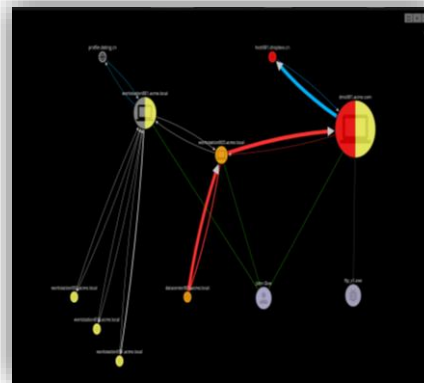
Methodologies

- Normalize
- Contextualize
- Relationships
- **Understand Data**

```
Artifact Detail View
message: "witfoo-artifact ::: streamName=CarbonBlack Protect Detection ::: clientIP=10.10.10.3 ::: d
message=millstone 8114 (Fig_v1.exe) found on dc0001.acme.local and executed by john@acme.com ::: 8114
::: severity=Critical ::: serverIP=111.14.36.195 ::: serverHostName=host001.drogon.co ::: serverType=
endTimestamp="2020-05-28 01:56:30"
timestamp: "5/28/20, 2:00 AM"
program: "CarbonBlack Protect Detection"
source: "localhost"
clientIP: "10.10.10.3"
clientHostName: "dc0001.acme.local"
clientBytes: "2763.57 KB"
clientPackets: -1
serverIP: "111.14.36.195"
serverHostName: "host001.drogon.co"
serverBytes: "149.31 KB"
serverPackets: -1
serverPort: 443
fileName: "Fig_v1.exe"
userName: "john@acme.com"
startTimeUTC: "2020-05-28 01:56:30"
endTimeUTC: "2020-05-28 01:56:30"
```

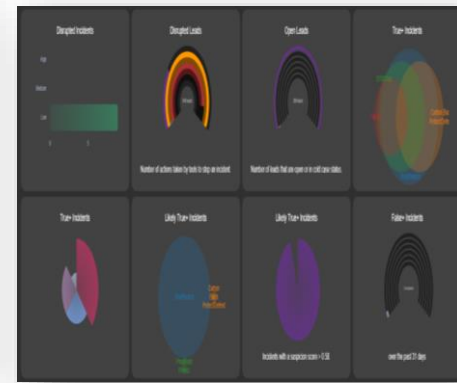
Artifact

- Semantic Frame
- Rule Based NLP
- *Intent* of Message
- **Normalized Search**



Incident

- Unit of Work
- Graph Theory
- Modus Operandi
- **Reduce MTTR**



Business Metrics

- GAP Accounting
- Tools & People
- Readiness Metrics
- **Reduce Incidents**

Artifact Creation

- **Comprehend** the message at receipt
- Rule-based Natural Language Processing (NLP)
- Semantic Framing for Normalization
- Determine “*Intent*” of Message
- Map fields to common schema/frame
- Associate Products
- Forensic preservation of original message
- Chain of Custody data
- Extreme speed (over Machine Learning NLP)

No Configuration Effort/Cost

Outsourced parsing maintenance



Unknown Msg

Sanitized Submission



WitFoo Library

Syslog

NetFlow

Agent

API

Kafka

Diverse Data

Hundreds of formats

witfoo

NLP (Rule Based)
Semantic Framing
Fast Fingerprinting



Artifact

Standardized Schema
Semantic Frame

Adaptive Parsing

WitFoo Artifact

Artifact Detail View

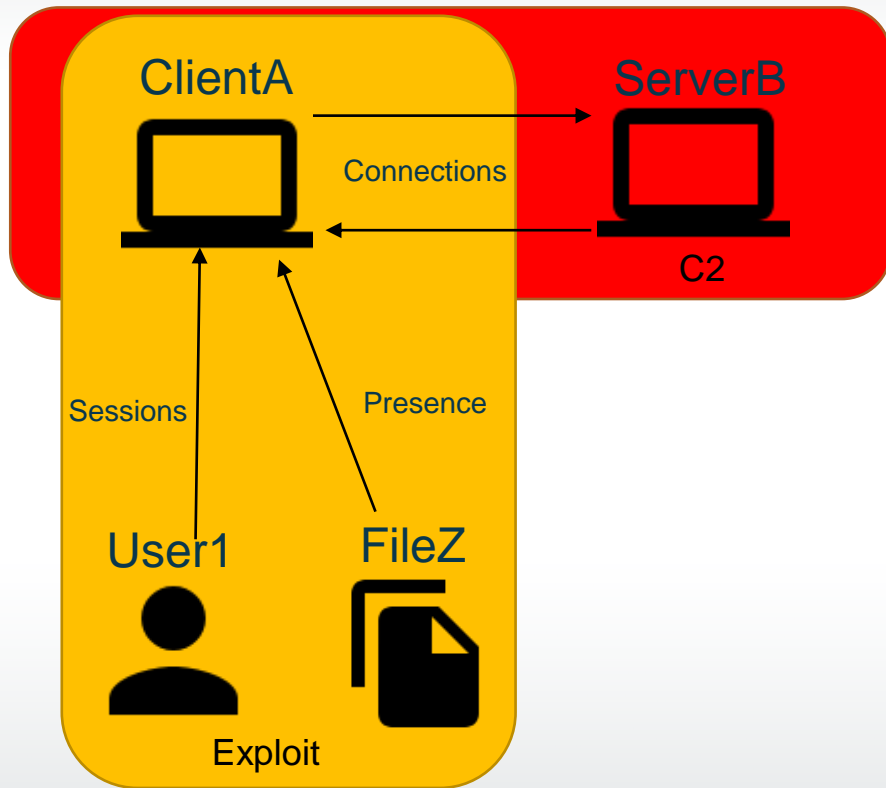
```
message: "WitFoo-Artifact ::: streamName=cisco_asa ::: clientIP=10.10.230.39 ::: startTimeUTC=2020-05-26 02:23:04 ::: endTimeUTC=2020-05-26 21:43:48 ::: message=cisco_asa ::: tags=[\"cisco_asa\", \"block\"] ::: action=deny ::: serverIP=9.10.33.75 ::: serverPort=32831 ::: protocol=6 ::: severityCode=3 ::: serverBytes=687582262481 ::: clientBytes=92253127082"
timestamp: "5/30/20, 2:15 AM"
program: "cisco_asa"
source: "localhost"
clientIP: "10.10.230.39"
clientHostname: ""
clientBytes: "85.92 GB"
clientPackets: -1
serverIP: "9.10.33.75"
serverHostname: ""
serverBytes: "640.36 GB"
serverPackets: -1
serverPort: 32831
startTimeUTC: "2020-05-26 02:23:04"
endTimeUTC: "2020-05-26 21:43:48"
protocol: 6
lat: 37.751
lng: -97.822
```

- Semantic Frame
- Standardized Schema
- 90+ Fields
- Product Mapping
- Intent Mapping
- Field Extraction
- Forensic Stamps
 - Transport
 - Source
 - Timestamps
 - Preservation of message
- *Consolidated Search*
- **Comprehended Unit of Evidence**

Incident Creation

- Fueled by Artifact Processing
- Nodes are computers, users and files/emails
- Edges are connections, sessions, file presences
- Nodes and Edges are updated by new artifacts
 - IP addresses, Byte counts, Packet counts, etc.
- Edges are evaluated for Modus Operandi behavior matches

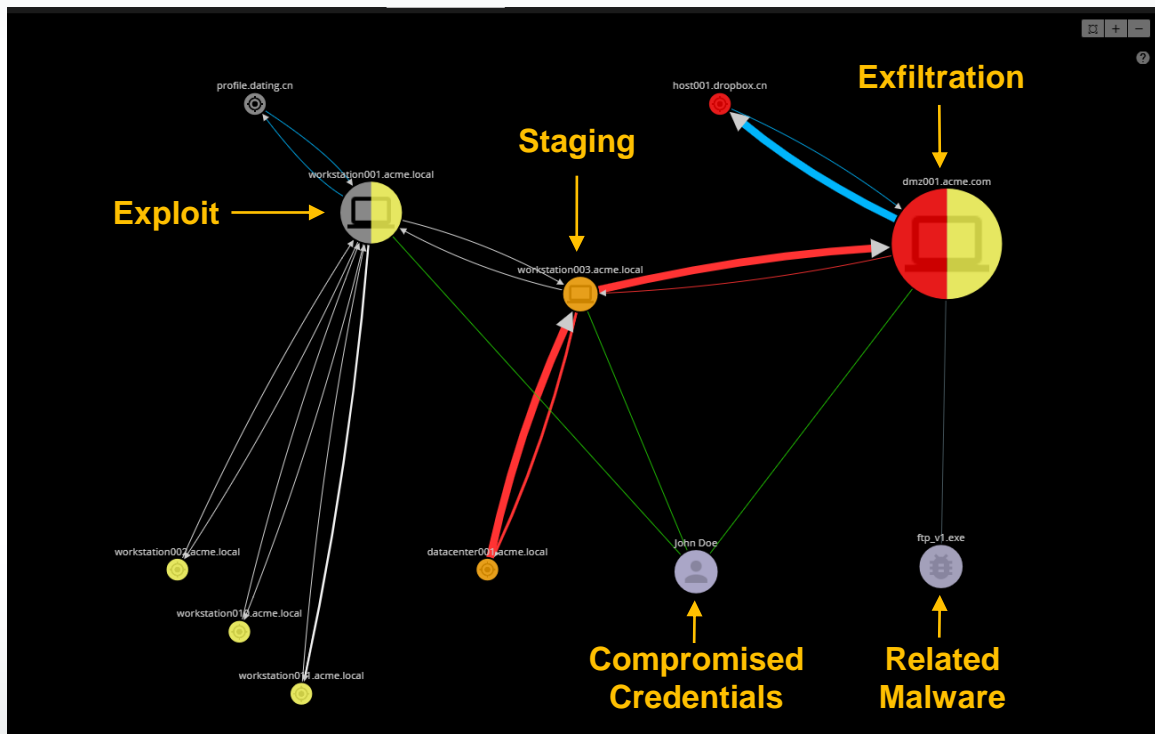
Graph Nodes & Edges



Artifacts
<ul style="list-style-type: none">• ClientName: ClientA• ClientIP: 10.10.10.43• ClientMAC: 00-DC-EF-23-15-12• Product: MS DHCP• MessageType: DHCP Lease• Intent: Asset Info
<ul style="list-style-type: none">• ClientName: ClientA• User: User1• File: FileZ• Product: Crowdstrike Falcon• MessageType: Malware Detected• Intent: Exploit Detection
<ul style="list-style-type: none">• ClientIP: 10.10.10.43• ServerName: ServerB• Product: Cisco Firepower• MessageType: C2 Detected• Intent: C2 Detection

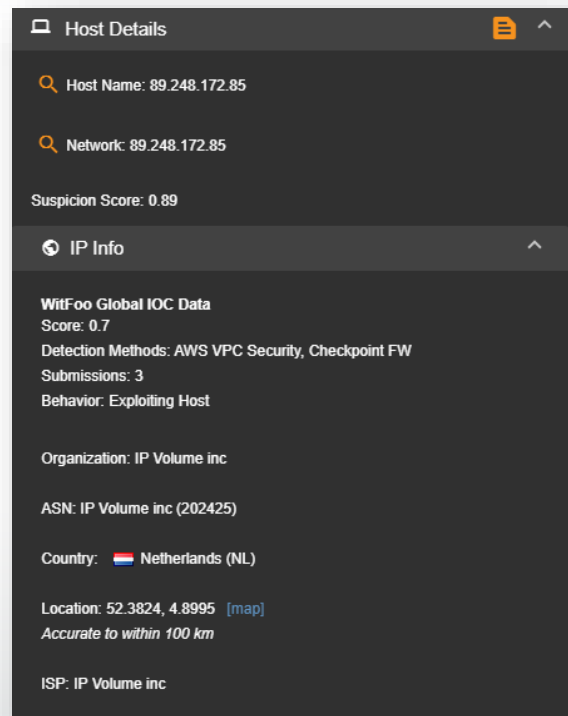
WitFoo Incident

- Patent Pending approach
- Meaningful Graph Relationships
- Modus Operandi of Attacker
- Combines, standardizes diverse data
- Learns from Investigator
- Consolidated Investigative unit
 - *Increases Clarity*
 - *Reduces Investigations*
 - *Reduces Time per Investigation*
- **Unit of Work**



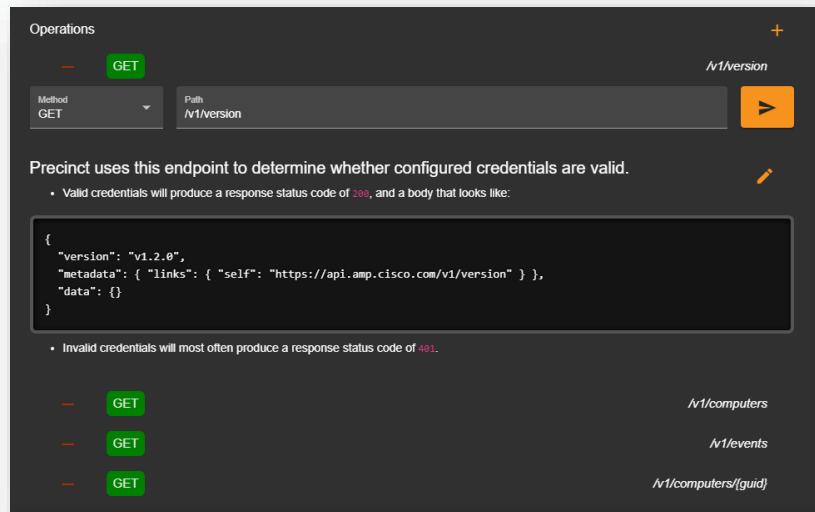
Global Indicator of Compromise Feed

- Anonymous Customer Submission
- Includes detection method/product
- Includes nefarious behavior types
- Includes suspicion score
- Retro-analysis of IOC hits
- Geo-IP Resolution
- ASN Resolution



Codeless Integrations

- Import OpenAPI Specification
- Published in WitFoo Library
- Support for REST & SOAP
- Code not required
- Amazon States Language Support
 - Developed by Amazon
 - States-language.net
 - JSON definitions of States Engines
- Custom WitFoo Precinct States Engine



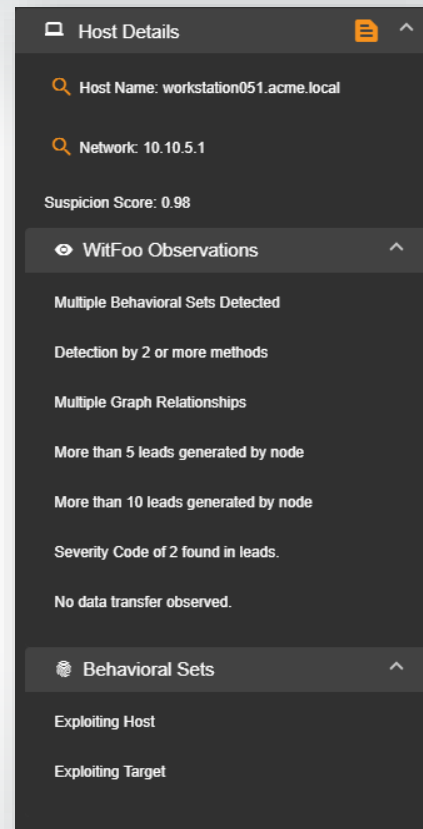
The screenshot displays the 'Operations' section of the WitFoo interface. At the top, there is a search bar with a green 'GET' button and a plus sign. Below this, a dropdown menu shows 'Method' as 'GET' and 'Path' as '/v1/version'. A yellow arrow button is to the right. The main content area contains a description: 'Precinct uses this endpoint to determine whether configured credentials are valid.' Below this, a bullet point states: 'Valid credentials will produce a response status code of 200, and a body that looks like:'. A code block shows a JSON response:

```
{  "version": "v1.2.0",  "metadata": { "links": { "self": "https://api.amp.cisco.com/v1/version" } },  "data": {} }
```

 Another bullet point below the code block states: 'Invalid credentials will most often produce a response status code of 401.' At the bottom, there is a list of other endpoints: 'GET /v1/computers', 'GET /v1/events', and 'GET /v1/computers/{guid}'.

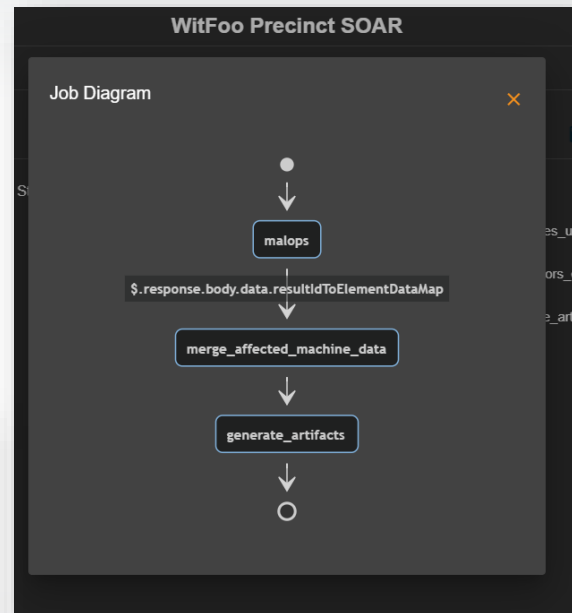
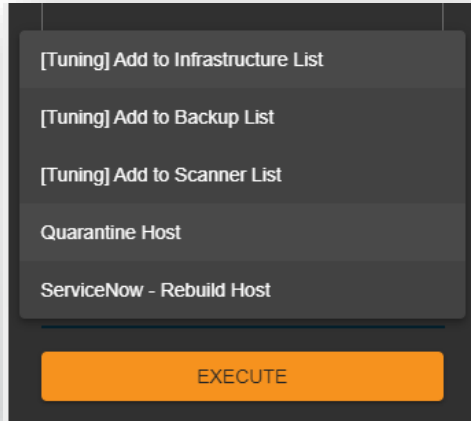
High-level SOAR

- Unit of Analysis: Incident
 - Context of Attack Type
 - State of all nodes & edges
 - All artifacts available
- Generalized Observations impact suspicion
- Suspicion approaches 1 when
 - Evidence Supports Modus Operandi Progression
 - Sufficient Evidence Exists
- Less Expensive to Maintain v. Linear SOAR
- More accurate than Linear SOAR

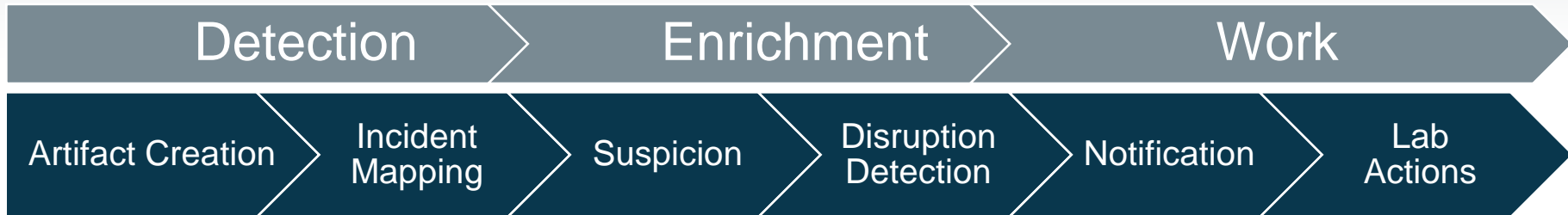


Codeless Response Jobs

- Collect External Data into Artifact
- Execute Playbooks
- Code not required
- Amazon States Language Support



WitFoo Incident Processing

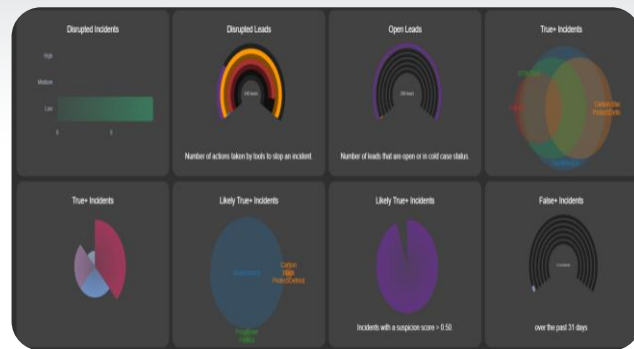


NLP (Rule Based) Semantic Framing Message Intent Message Source Frame = Artifact	Graph Theory Modus Operandi Behavior Analysis UEBA + IOC Unit of work	Crowdsourced Org Specific Expert Insights Eliminate False + Sufficient evidence	Monitor Evidence Understand Block Verify Disruption	Email Webhook Ticket	RBAC Controlled JSON Playbooks Automatic/Manual Crowdsourced OOTB Integrations
--	---	---	---	----------------------------	--

- Only High Suspicion, non-Disrupted (HSND) incidents require human investigation
- After achieving 3.5+ WitFoo Readiness Score, most deployments have less than 10 HSND/month
- Manual Lab actions allow for audited, controlled remediation actions

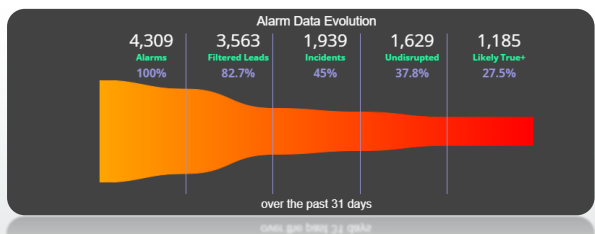
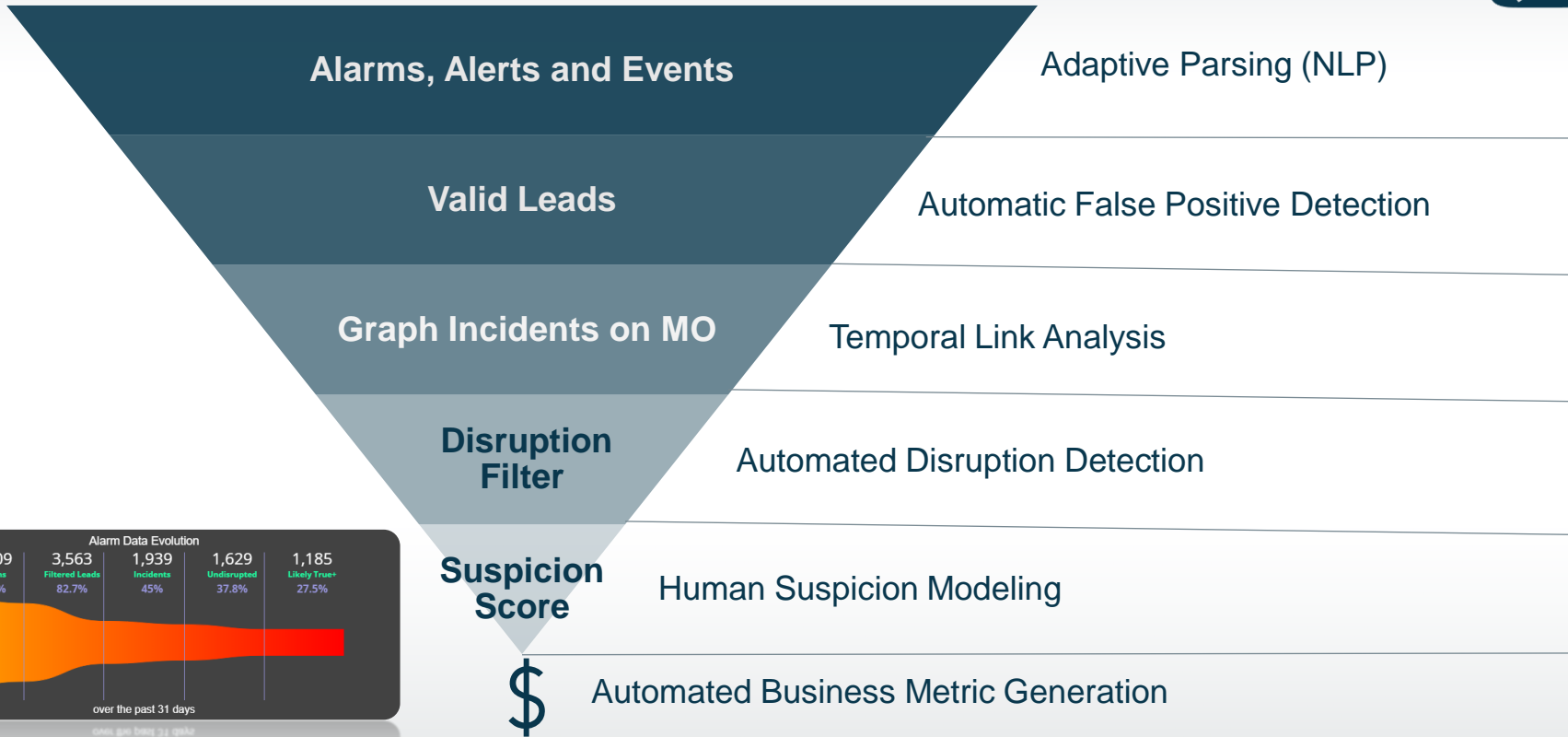
WitFoo Report Generation

- Analyzes Incidents (Unit of Work)
 - By Product
 - By Modus Operandi
 - By Status
 - By Personnel
 - By Critical Security Controls
- Reports are fully updated hourly



CID/ID	DESCRIPTION	PRODUCT	REFERENCE
1	▲ 92% Inventory and Control of Hardware Assets (ITMANAC)	Carbon Black Protect/Defend/Falcon/Qualys VM	100.00.00.00
2	▲ 92% Inventory and Control of Software Assets (Application Whitelisting)	Qualys VM, Falcon, Carbon Black Protect/Defend	100.00.00.00
3	▲ 91% Continuous Vulnerability Management (Vulnerability Patch Management)	Qualys VM	100.00.00.00
4	● 80% Controlled Use of Administrative Privileges (Authentication/Authorization)		100.00.00.00
5	▲ 80% Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	Qualys VM, Falcon, Carbon Black Protect/Defend	100.00.00.00
6	✓ 100% Maintenance, Monitoring and Analysis of Audit Logs	Protecd	100.00.00.00
7	● 80% Email and Web Browser Protections	ProofPoint Protect	100.00.00.00
8	▲ 80% Malware Defenses	Carbon Black Protect/Defend/Falcon	100.00.00.00
9	▲ 80% Limitation and Control of Network Ports, Protocols and Services	ASA Firewall	100.00.00.00
10	● 80% Data Recovery Capabilities		100.00.00.00
11	▲ 80% Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	Qualys VM	100.00.00.00
12	✓ 100% Boundary Defense	Snafwhatch, ASA Firewall	100.00.00.00
13	▲ 80% Data Protection	Snafwhatch	100.00.00.00
14	● 80% Controlled Access Based on the Need to Know		100.00.00.00

WitFoo Unique Innovations



WitFoo Aggregation Mode

- Incidents, Reports, Rules
- Issue Search & SOAR Jobs
- One-way HTTPS Connection
- Queuing for poor Internet
- No limit on aggregators

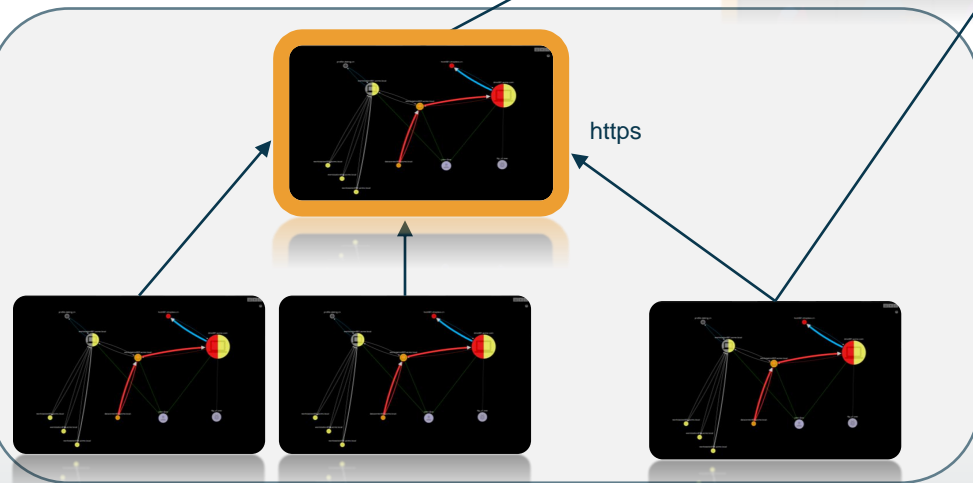


Aggregate Reporting

- Cybersecurity Insurers
- Vendor Management
- Ongoing Audit
- Chain-of-Command

Aggregate Operations

- MSSP
- Military SOC
- Community SOC
- M&A
- Report to Law Enforcement



Precinct Architecture

Deployment Options



Microsoft
Hyper-v



openstack.



VirtualBox

Hypervisors



Custom Build



Managed Service



ORACLE



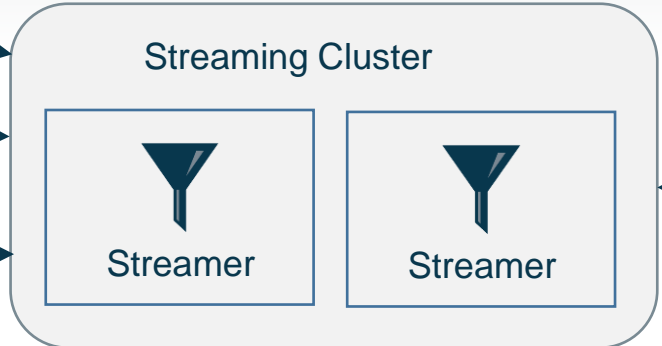
Cloud Hosted

Horizontally Scalable

Syslog
514/udp/tcp
6514/tls

NetFlow
2055/udp

Beats
5044/tls



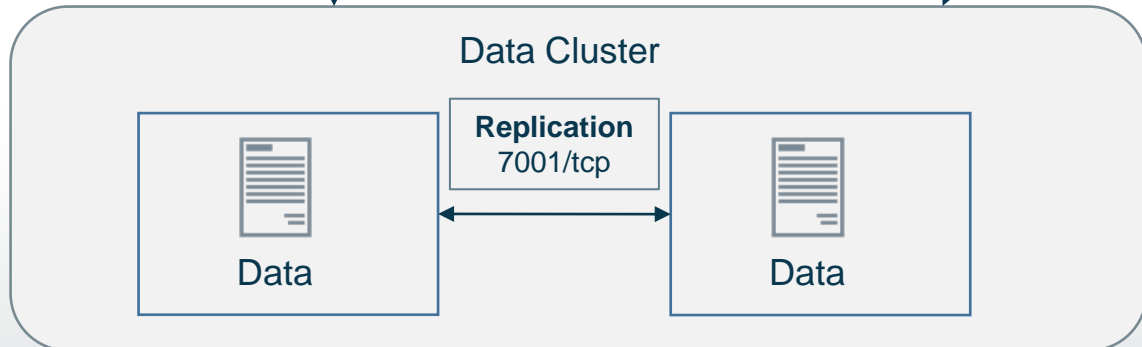
API
443/tls



HTTPS
443/tcp



Cassandra
9042/tcp



Horizontal Scale

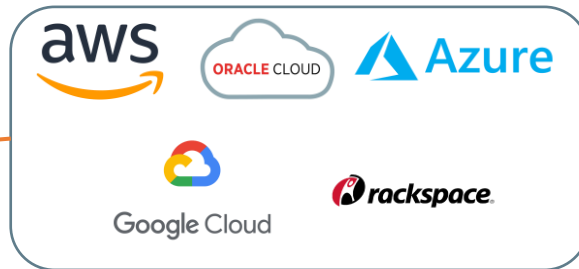
- DC Aware Replication
- Load Balanced
- Cloud Assist Config
- Slow Disk OK
- Also Vertically Scalable

WitFoo Precinct Cloud Visibility

Deploy Appliances in Cloud



Send Syslog, NetFlow, Agent Data



Import Analytics via API



Market Strategy

Market Philosophies

- Existing products are overpriced vs. derived value
- Market bubble will “pop”
- Pricing needs to be cost-contained to customer-controlled value
- Valuable Partners should be protected in closing deals
- Sustainable sales are built on Distribution -> Resell model
- Enabled Reselling Partners reduce cost of sale and support
- Enabled Reselling Partners enable scale
- Enabled Reselling Partners maximize value to customers
- Professional Services = unfinished product

Go to Market Strategy

- Pure Channel
 - Ease of Sell
 - Guaranteed Margin
 - Assessment Pull
 - Low cost of support
- OEM Selling
- Technical Co-branding
- Transparency/Low Sale Cost
- Enablement Portal



Westcon  Comstor

 amazon
web services

 Microsoft Azure

 NEXUS We Mean Security

 structured
bridging people, business & technology

 OPTIV

 BORDERHAWK
CyberSecurity

 RSI

 Cumberland
GROUP

 BlackBerry |  CYLANCE

 f5

 ORACLE

 CISCO

 CROWDSTRIKE

 Gigamon

 Carbon Black.

Early Sales Progress

Early Customers



- **Customer validated technology**
- **Sustainable, Partner-driven sales**
- Opportunity growth-rate exponential
- \$380k ARR on 8/30/2020
- Public sector, enterprise & mid-market

Market Comparison

Disclaimer: *This information was compiled by WitFoo competitive research and has not been fact-checked by competing organizations.*

Purchasing Considerations

	 witfoo	 splunk	 sumologic	 exabeam	 DEVO	 SECURONIX
Cost-contained	✓			✓		
Affordable to mid-market	✓		✓			
Turn-key deployment	✓					
Executive Comprehension of Security	✓					
Investigator Comprehension	✓			✓		✓
Simple Search of Data	✓	✓	✓	✓	✓	✓
Flexible Deployment Options	✓	✓				
Ease to Purchase	✓	✓		✓		
SOAR	✓	✓	✓			✓
UEBA	Roadmap	✓	✓	✓		✓

Technology Comparison

	witfoo	splunk>	+ sumologic	exabeam	DEVO	SECURONIX
Custom Dashboards	Roadmap	✓	✓	✓	✓	✓
Big Data Search	✓	✓	✓		✓	✓
Modus Operandi Analytics	✓	Entity		Entity		Entity
Global Threat Feed	✓					
High-level SOAR	✓	Low-level				Low-level
Data Normalized	✓					✓
Adaptive Parsing	✓	Community				
Business Metrics	✓					
Turn-key deployment	✓	High Effort	High Effort	High Effort	Medium Effort	Medium Effort

Business Comparison

	witfoo	splunk	sumologic	exabeam	DEVO	SECURONIX
Cost-contained Pricing	✓	Data	Data	✓	Data	Data
On-prem deployment	✓	✓	✓	✓		
SaaS	Via Partners	✓	✓		✓	✓
Amazon Cloud	✓	✓				
Microsoft Cloud	✓	✓				
Global Distributor	✓	✓	✓	✓		
Partner Network	✓	Direct First	Direct First	Direct First		Direct First
Direct Sales	Channel Driven	✓	✓	✓	✓	✓
Mid-market	✓		✓			

WitFoo Advantages vs. Splunk*

- Cost-contained license model (#1 complaint against Splunk)
- Adaptive parsing not requiring FTE to maintain (#2 complaint)
- Accessibility to mid-market and SMB (#3 complaint)
- Industry's most attractive Channel Program
- Infinite horizontal scale with lowest IOPS requirements
- Industry's first **diagnostic SIEM** (security business metrics)
- WitFoo Global IOC (Community driven threat feed)
- Recessed market will seek a turnkey, cost-contained solution

Customer Success

Scalable Customer Success

- Monitored Metrics
- Cloud Assisted Config
- Free Training
- Engaged Partners
- Custom Definitions

 WitFoo Library APP 10:44 AM
The Ma [redacted] precinct deployment on VM: log-ic1.oh [redacted] has system issues. Expected 0.98 or less CPU Use. Got 0.9895 see <https://metrics.witfoo.com/app/kibana#/dashboard/79ff6e0-faa0-11e6-947f-1771697178b8> for more details.



The screenshot shows a Gartner Peer Insights review for WitFoo Precinct. The review title is "Overall A Good Product. WitFoo Support Is Exceptional." and it was submitted on September 23, 2020. The overall user rating is 5 stars. The reviewer provided an overall comment: "WitFoo Precinct is a good all around product for threat monitoring, alerting and network visibility in a single pane of glass." The review also includes ratings for various categories: Evaluation & Contracting (5 stars), Integration & Deployment (4 stars), Service & Support (5 stars), and Product Capabilities (4 stars).



Code
Releases

Customer
Metrics

Integration
Signatures

Semantic
Frames

SOAR Jobs

IOC Data

Licensing



Support
Tickets

Integration
Guides

Feature
Requests

Release
Notes

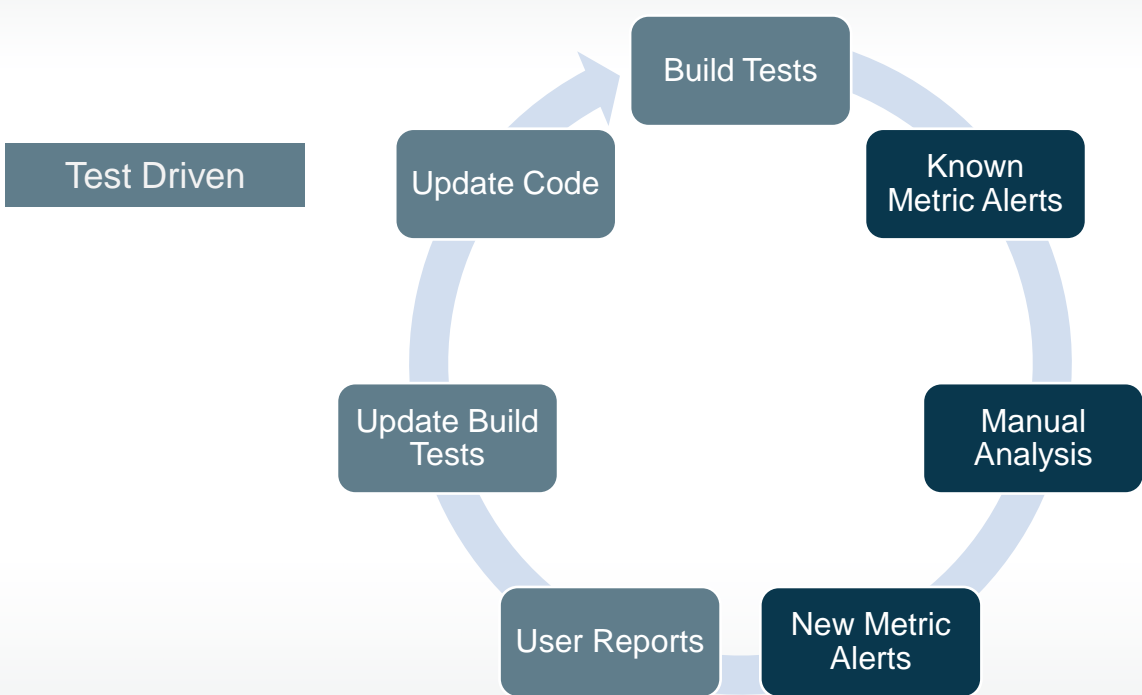
Forums

Training

Slack Access

Development Methodology

Metric Driven Development



- Thousands of metrics each minute reported to WitFoo Library for analysis
- Rapid detection of issues in the field
- Rapid testing of patches to effected deployments
- Validation of hypotheses
- Feature impact on other features and stability

Metric Driven

Summary

Key Takeaways

- Business Metrics
- Predictive Diagnostics
- Data **Comprehension**
- Codeless SOAR
- Simple Data Search
- Federated Data Sharing
- High-Fidelity IOC Feed
- Infinite Big-Data Scale
- Free trials
- Integrations Included in Pricing
- Hagggle-free, Cost-contained Pricing
- Channel-only Sales
- Monitoring Included in Pricing
- SaaS, On-Prem, Cloud, MSSP
- Simple Procurement
- No Professional Services
- World-class Customer Support

witfoo